CCMS V3 E-Filing CCTC-EFSP Connectivity Technical Guide

AUGUST 2010

ADMINISTRATIVE OFFICE OF THE COURTS
INFORMATION SERVICES DIVISION

Judicial Council of California
Administrative Office of the Courts
Information Services Division
455 Golden Gate Avenue
San Francisco, CA 94102-3688

Table of Contents

Revision History

This section includes this documents' revision history:

Version	Date	Editor	Changes	Sections
1.0	3/15/2010	Todd Vincent, <xmlLegal>, Spring Snuffin	Final document prepared from internal versions. Changed fonts and styles to match AOC format.	All Sections.
1.1	8/9/2010	Todd Vincent, <xmlLegal>	Changed made based on comments from Edmund Herbert, Pamela Sampson-Smith, Raj Talla, and Robert Riedel.	Introduction, Section 1, Section 2, Section 4, and Section 6.
1.1	8/23/2010	Todd Vincent, <xmlLegal>	Changed document date only.	

Introduction

The document's intended audience includes Electronic Filing Service Providers (EFSP) who are authorized to electronically file into the California Case Management System, Version 3 (CCMS or CCMS V3).

This is a technical and support document. The purpose of this document is to provide instructions and support information to authorized EFSPs for connectivity to the California Courts Technology Center (CCTC) CCMS V3 Electronic Filing Manager (EFM). The document also includes information about testing connectivity once established. The document may also be used as a guideline for connectivity to local implementations of the CCMS EFM in non-CCTC courts.

Section 1 overviews the CCMS V3 E-Filing System and reminds EFSPs that legal agreements must be signed prior to connecting to the CCTC environment.

Section 2 states technical connectivity requirements for both ingress and egress connections. For the sake of clarity and completeness, this section includes negative requirements.

Section 3 lists and briefly describes the AOC / CCTC test environments into which the EFSP will connect. Test environments are mapped to test phases, which use similar but slightly different terminology. Environments describes are Pre-Production Test, Staging, and Production.

Section 4 includes an EFSP check list. This check list is intended to provide EFSPs with an easy-to-understand, chronological list of activities both before and after connectivity.

Finally, Section 5 includes information about Help Desk Support.

This document includes requirements and policies that are applicable to CCMS V3. These requirements and policies may be different for CCMS V4.

1. Overview

1.1. CCMS V3 E-Filing System

The CCMS V3 E-Filing System includes EFM and Clerk Review software components (e-filing system). The e-filing system is implemented in the CCTC (CCTC implementation) and in individual courts (local court implementations). The CCTC is a data center maintained by the California Administrative Office of the Courts (AOC).

The CCTC implementation supports multiple courts (e.g., Ventura, Sacramento, and San Joaquin) at the same time using the same instance of the CCMS EFM. Local court implementations typically support only one court at a time (e.g., Orange, San Diego separately). For example, Sacramento county and Ventura county both operate from the CCMS EFM located in CCTC, whereas Orange county operates individually from a local CCMS EFM implementation installed in Orange county.

This document specifies requirements for connectivity to the CCTC implementation. Local court implementations may support similar connections, but may also have some variations on a court-by-court basis. Consult with the court for specific requirements of local court implementations.

1.2. CCTC Supports Multiple Electronic Filing Service Providers

The CCMS V3 e-filing system supports multiple third party EFSPs. EFSPs have the ability to electronically file into both the CCTC implementation and local court implementations provided the EFSP is authorized to connect and electronically file.

The EFSPs are considered authorized to connect and electronically file into the CCTC implementation once they sign the CCTC E-Filing Access Agreement.

1.3. Legal Agreements

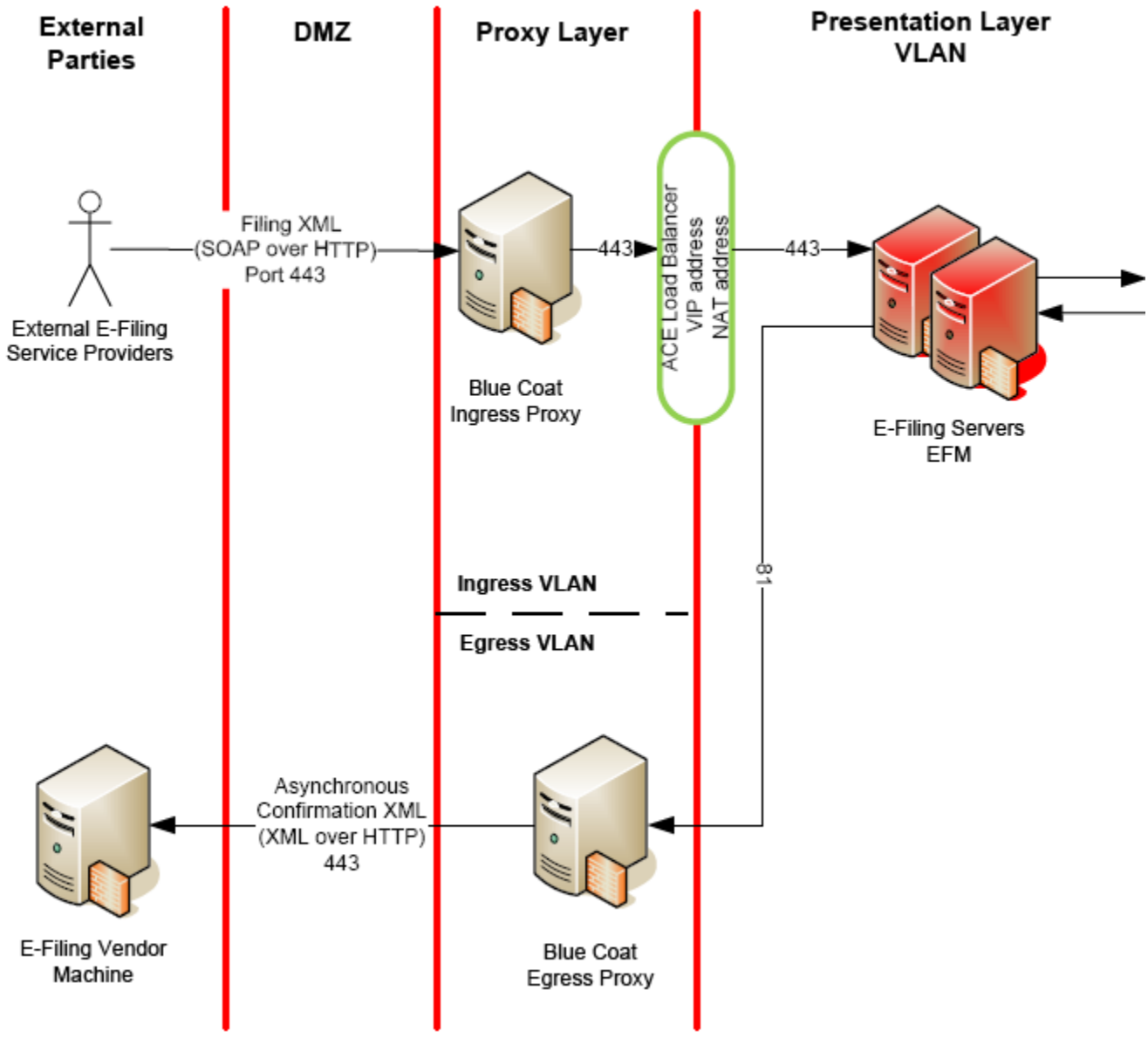
There are at least two legal agreements that EFSPs must sign prior to accessing the CCTC environment.

- All EFSPs are required to sign the ***AOC-CCTC-EFSP E-Filing Connectivity Agreement*** for connectivity into the CCTC. The legal agreement must be executed before EFSP will be allowed to make technical connections.
- EFSPs must also sign a ***Court-EFSP Electronic Filing Legal Agreement*** or a ***Statewide AOC-EFSP Electronic Filing Legal Agreement***.

With these agreements in place, the EFSP is authorized to connect to the CCTC environment. Contact the AOC or a local court for additional information.

2. Connectivity Requirements

This section defines technical requirements for incoming connectivity to the CCTC and the EFM and outgoing connectivity from the CCTC and the EFM. Incoming connectivity is for EFSPs to submit filings to the courts (Filing XML in the following graphic). Outgoing connectivity is for the courts to send asynchronous confirmations to EFSPs (Asynchronous Confirmation XML in the following graphic).



2.1. Incoming Connectivity (Filings)

This section specifies requirements for *incoming* CCTC connectivity. Incoming CCTC connectivity is required to submit filings into the EFM.

2.1.1. Authentication and IP Filtering

CCTC does not require authentication to submit transactions into the EFM. CCTC uses IP filtering in the network firewall. Therefore, EFSPs must submit one or more incoming IP addresses to their sponsor court or to their AOC representative. The court or the AOC will provide the IP address to the CCTC, which will in turn enable ingress firewall access. The court or the AOC will then arrange a time to test the connection with the EFSP. CCTC does not use or issue client certificates to EFSPs to authenticate EFSPs for inbound transmission. CCTC does not use authentication on the web server.

The CCMS EFM requires the Filing XML to include a registered organization key. The organization key is used to identify the EFSP to the EFM. See Section 3.1 of the CCMS-2GEFS Implementation Guide for additional information.

2.1.2. Security Sockets Layer (SSL)

The CCTC requires industry standard Secure Sockets Layer (SSL) over HTTP for encrypted communication into the CCTC. CCTC uses the standard SSL port 443. CCTC uses a well-known root Certificate Authority for SSL server certificates (i.e., Entrust).[1] Accordingly, EFSPs should have, or be able to obtain, necessary public root certificates for communicating with CCTC using SSL over HTTP.

2.1.3. SOAP, WSDL, 2GEFS Envelope

The CCMS EFM uses SOAP over HTTP(S) to for transmitting valid 2GEFS Filing XML. The SOAP web service is defined by a WSDL file. See Section 1.1 of the CCMS-2GEFS Implementation Guide for additional information.

2.2. Outgoing Connectivity (Asynchronous Confirmations)

This section specifies requirements for *outgoing* CCTC connectivity. Outgoing connectivity is required for the EFM to submit asynchronous confirmations to the EFSP.

[1] By end of year 2010, CCTC policy is to use an Entrust SSL certificate using 2048 bit SSL encryption. This is in compliance with mandates from the United States National Institute of Standards and Technology (NIST).

2.2.1. Authentication and IP Filtering

CCTC security policy requires the IP filtering for outgoing communications. As a result, the EFSP must submit one or more IP addresses to their sponsor court or their AOC representative. The court or the AOC will provide the IP address to the CCTC, which will in turn enable egress firewall access. The court or the AOC will then arrange a time to test the connection with the EFSP. .

The EFM application supports dynamic "reply to" addresses. While the EFM application supports fully dynamic addresses, the IP filtering limits the ability to use any reply to address. The reply to address must contain either a fully qualified domain name associated with an IP address or an IP address configured in the CCTC firewall. See Section 2.2 of the CCMS-2GEFS Implementation Guide for additional information.

EFSP must not use certificate based authentication or web server authentication in their receiving systems.

2.2.2. Security Sockets Layer (SSL)

The CCTC requires industry standard Secure Sockets Layer (SSL) over HTTP for encrypted communication out of the CCTC. CCTC are expected to use the standard SSL port 443. EFSPs are expected to use a well-known root Certificate Authority for SSL server certificates (e.g., VeriSign or Entrust). CCTC will not accept self-signed certificates or certificates from an obscure Certification Authority.

2.2.3. SOAP, WSDL, 2GEFS Envelope

The CCMS EFM uses XML over HTTP(S) to send valid 2GEFS (Asynchronous) Confirmation XML out of CCTC to the EFSP. EFSPs must receive XML over HTTP(S) from the EFM. EFSPs cannot implement SOAP web services to receive asynchronous confirmations. See Section 1.1 of the CCMS-2GEFS Implementation Guide for additional information.

3. Test Phases and Environments

CCTC implementations use the following terminology to describe pre-production and production test phases and test environments. A test phase is an activity. A test environment is a technical implementation of a network, hardware, and software.

The test phases include:

- ***User Acceptance Testing (UAT)***
- ***Certification Testing***
- ***Production***

The test environments include:

- ***User Acceptance Testing (UAT)***: Pre-Production environment for UAT testing.
- ***Localization Test (LT)***: Pre-Production environment for UAT testing.
- ***Staging***: Pre-Production environment for Certification testing.
- ***Production***: Live filings occur in the production environment.

The information in this section includes typical information about these environments. Your AOC or CCTC representative will have additional information about the environment into which you will test.

Local court implementations may have different environments and naming conventions. Local court implementations (i.e., non-CCTC implementations) will have different test and production URLs.

3.1. Pre-Production Test Environment

EFSPs will have access to the court's test environment via the CCTC. Testing is intended to focus on testing the system for business and operational issues. The focus is less on technical testing, which has been done in earlier test phases.

Testing may occur in either the UAT or the LT environment. Do not confuse the UAT test phase with the UAT and LT environments.

The court or courts will provide service providers with URLs for the test environment or environments into which the service provider is to test.

3.2. Staging Environment

Once an EFSP satisfies the court's UAT requirements, the EFSP is promoted to the court's staging environment for certification testing. Certification testing is performed in the Staging environment prior to deployment to Production to certify the release package and its deployment procedures.

There will be a separate URL for gaining access to the Staging environment. The court or courts will provide service providers with URLs for the Staging environment into which the service provider is to test.

3.3. Production Environment

EFSPs will have access to a court's production environment following certification testing. Validation testing may be conducted in the production environment immediately after an EFSP is promoted from stating to production and from time-to-time as needed. Production validation is limited by lack of test data and inability to enter/delete court cases.

There will be a separate URL for gaining access to production environment. The court or courts will provide service providers with production URLs.

4. EFSP Checklist

The following table provides a checklist of high-level activities an EFSP should accomplish in anticipation of electronically filing into CCMS courts.

Name	Description
Selection	An EFSP must be selected by a California court to participate in CCMS electronic filing.
Contracting (Court)	An EFSP must negotiate and sign a legal agreement with the court. See Section 6.
Contracting (AOC-CCTC)	For courts hosted in the CCTC, an EFSP must sign a legal agreement with the AOC. See Section 6.
Development	An EFSP must develop an e-filing solution based on the AOC and CCMS e-filing standards. See Section 6.
<xmlLegal> Test Suite Testing (Optional)	Optionally, an EFSP may test its solution by filing into the <xmlLegal> Test Suite EFM application. This testing will provide basic compliance information to the EFSP prior to connecting to the court's environment. Contact your AOC representative for additional information.
UAT Testing	An EFSP must participate in and pass UAT testing. See Section 3.1.
Certification Testing	An EFSP must participate in and pass Certification testing. See Section 3.2.
Production Validation	An EFSP must participate in and pass production validation testing. See Section 3.3.
Go Live	Following the steps above, the EFSP is ready to file live filings into CCMS.

5. Help Desk Support

This section outlines AOC, CCMS, and CCTC Help Desk support available for EFSPs.

5.1. Help Desk Support

The CCTC Help Desk provides courts supported services related to technical and E-Filing issues as encountered by the courts. EFSPs must go through their respective courts to open a ticket with the CCTC Help Desk.

5.2. Help Desk Support Hours

Existing Help Desk support hours for CCTC are as follows:

- Help Desk Support Hours:
    - M-F 7am-7pm, excluding court holidays.
- After Hour Help Desk Support:
    - Courts can leave voicemail with the Help Desk outside the support hours; this message is then dispatched to afterhours support.

6. Associated Documentation

This section outlines documentation associated with this technical guide and relevant to EFSPs. If you are an EFSP and you have received this document, you should have all of the documents listed below. If you do not have all of the documents listed below, contact your sponsoring court or your AOC representative.

- Court-EFSP Electronic Filing Legal Agreement
- AOC-CCTC-EFSP E-Filing Connectivity Agreement
- CCTC-EFSP Connectivity Technical Guide (this document)
- Court Policy (or Policies) for Specific Courts
- CCMS-2GEFS Implementation Guide
- 2GEFS-CCMS 01 to 02 Schema Updates
- 2GEFS Schemas and Documentation